STATE OF ALABAMA

Information Technology Standard

Standard 680-01S3: Removable Storage Devices

1. INTRODUCTION:

Removable non-volatile storage devices (USB Flash drives, PC Cards, FireWire devices, MP3 players, camcorders, digital cameras, etc.) have the same vulnerabilities as disk media (malware, data loss) but greater capacity, and could be used to infect an information system (IS) to which they are attached with malicious code, could be used to transport sensitive data leading to potential compromise of the data, and are frequently lost or stolen. Careful attention to the security of such devices is necessary to protect the data they may contain.

2. OBJECTIVE:

Protect State data from loss.

3. SCOPE:

These requirements apply to all users (State of Alabama employees, contractors, vendors, and business partners) of any removable storage device that could be attached to any State-managed IS resource.

4. REQUIREMENTS:

> *Policy: Ensure appropriate levels of protection are applied to information resources by developing standards and procedures for determining and implementing minimum security requirements based on the information protection category.*

No removable storage device shall be attached to a State IS unless approved by the IT Manager. The IT Manager shall maintain an inventory of all approved removable storage devices and ensure controls are in place to protect the confidentiality, integrity, and availability of State data.

Removable non-volatile storage devices shall be secured, marked, transported, and sanitized as required by State standards in the manner appropriate for the data category they contain.

Removable non-volatile storage devices shall, whenever possible, be formatted in a manner that allows the application of Access Controls to files or data stored on the device.

Sensitive or confidential data shall not be stored on any removable non-volatile storage device unless encrypted in accordance with applicable State standards. For devices that do not support encryption of the storage media, sensitive and confidential data shall, as promptly as possible, be transferred to a device that does support the required encryption and access controls. In the interim, the device shall be securely stored apart from its storage media (whenever possible) and physical security must be assured. Organizational procedures shall

clearly define the handling requirements for such data and devices, and device users shall be made aware of the risks and procedures.

No IS shall have its BIOS set to allow a boot from any removable storage device (exception: an IS can be booted from a removable storage device for maintenance or recovery purposes only). The auto-run feature shall be disabled on all ports used by removable storage devices (USB, FireWire, PC Card readers, etc).

Users shall virus-scan all portable storage media (diskettes, CDs, USB drives, etc.) before files residing on the media are transferred or accessed.

Maintain physical security of removable storage devices. Report immediately the loss or theft of any device containing any State data.

User awareness training shall describe the risks and threats associated with the use of removable storage devices, the handling and labeling of these devices, and a discussion of the devices that contain persistent non-removable memory.

5. DEFINITIONS:

6. ADDITIONAL INFORMATION:

6.1 POLICY

Information Technology Policy 680-01: Information Protection

6.2 RELATED DOCUMENTS

Information Technology Standard 680-01S1: Information Protection

Information Technology Standard 680-03S1: Encryption

Signed by Eugene J. Akers, Ph.D., Assistant Director

7. DOCUMENT HISTORY:

Version	Release Date	Comments
Original	12/12/2006	